[Discussion Draft]

AMENDMENT TO H. RES. 164

OFFERED BY M__. _____

At the end of the resolution, add the following:

SEC. 2. Notwithstanding any other provision of this resolution, the amendment specified in section 3 shall be in order as though printed as the last amendment in House Report 113–41 if offered by Representative McCaul of Texas or his designee. That amendment shall be debatable for 10 minutes equally divided and controlled by the proponent and an opponent.

SEC. 3. The amendment referred to in section 2 is as follows: After section 1, insert the following new section (and renumber subsequent sections accordingly):

"SEC. 2. FEDERAL GOVERNMENT COORDINATION WITH RESPECT TO CYBERSECURITY.

''(a) COORDINATED ACTIVITIES.—The Federal Government shall conduct cybersecurity activities to provide shared situational awareness that enables integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents.

''(b) COORDINATED INFORMATION SHARING.—

''(1) DESIGNATION OF COORDINATING ENTITY FOR CYBER THREAT INFORMATION.—The President shall designate an entity within the Department of Homeland Security as the civilian Federal entity to receive cyber threat information that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, except as provided in paragraph (2) and subject to the procedures established under paragraph (4).

''(2) DESIGNATION OF A COORDINATING ENTITY FOR CYBERSECURITY CRIMES.—The President shall designate an entity within the Department of Justice as the civilian Federal entity to receive cyber threat information related to cybersecurity crimes that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, subject to the procedures under paragraph (4).

''(3) SHARING BY COORDINATING ENTITIES.—The entities designated under paragraphs (1) and (2) shall share cyber threat information shared with such entities in accordance with section 1104(b) of the National Security Act of 1947, as added by sec-

tion 3(a) of this Act, consistent with the procedures established under paragraphs (4) and (5).

''(4) PROCEDURES.—Each department or agency of the Federal Government receiving cyber threat information shared in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, shall establish procedures to—

''(A) ensure that cyber threat information shared with departments or agencies of the Federal Government in accordance with such section 1104(b) is also shared with appropriate departments and agencies of the Federal Government with a national security mission in real time;

''(B) ensure the distribution to other departments and agencies of the Federal Government of cyber threat information in real time; and

''(C) facilitate information sharing, interaction, and collaboration among and between the Federal Government; State, local, tribal, and territorial governments; and cybersecurity providers and self-protected entities.

''(5) PRIVACY AND CIVIL LIBERTIES.—

"(A) POLICIES AND PROCEDURES.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act. Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

"(i) minimize the impact on privacy and civil liberties;

"(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

"(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to identify

specific persons from unauthorized access or acquisition;

''(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

''(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

''(B) SUBMISSION TO CONGRESS.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall, consistent with the need to protect sources and methods, jointly submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

''(C) IMPLEMENTATION.—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under such section 1104(b) shall—

''(i) implement the policies and procedures established under subparagraph (A); and

''(ii) promptly notify the Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, the Secretary of Defense, and the appropriate congressional committees of any significant violations of such policies and procedures.

''(D) OVERSIGHT.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

''(6) INFORMATION SHARING RELATIONSHIPS.—Nothing in this section shall be construed to—

''(A) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Defense and an entity that is part of the defense industrial base;

''(B) alter existing information-sharing relationships between a cybersecurity provider, protected entity, or self-protected entity and the Federal Government;

''(C) prohibit the sharing of cyber threat information directly with a department or agency of the Federal Government for criminal investigative purposes related to crimes described in section 1104(c)(1) of the National Security Act of 1947, as added by section 3(a) of this Act; or

''(D) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Treasury and an entity that is part of the financial services sector.

''(7) TECHNICAL ASSISTANCE.—

''(A) DISCUSSIONS AND ASSISTANCE.—Nothing in this section shall be construed to prohibit any department or agency of the Federal Government from engaging in formal or informal technical discussion regarding cyber threat information with a cybersecurity provider or self-protected entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such a provider or such an entity.

''(B) COORDINATION.—Any department or agency of the Federal Government engaging in

an activity referred to in subparagraph (A) shall coordinate such activity with the entity of the Department of Homeland Security designated under paragraph (1) and share all significant information resulting from such activity with such entity and all other appropriate departments and agencies of the Federal Government.

''(C) SHARING BY DESIGNATED ENTITY.—Consistent with the policies and procedures established under paragraph (5), the entity of the Department of Homeland Security designated under paragraph (1) shall share with all appropriate departments and agencies of the Federal Government all significant information resulting from—

''(i) formal or informal technical discussions between such entity of the Department of Homeland Security and a cybersecurity provider or self-protected entity about cyber threat information; or

''(ii) any technical assistance such entity of the Department of Homeland Security provides to such cybersecurity provider

or such self-protected entity to address vulnerabilities or mitigate threats.

''(c) REPORTS ON INFORMATION SHARING.—

''(1) INSPECTOR GENERAL OF THE DEPARTMENT OF HOMELAND SECURITY REPORT.—The Inspector General of the Department of Homeland Security, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the appropriate congressional committees a report containing a review of the use of information shared with the Federal Government under subsection (b) of section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act, including—

''(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

''(B) a review of the type of information shared with the Federal Government under such subsection;

''(C) a review of the actions taken by the Federal Government based on such information;

''(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;

''(E) a list of the departments or agencies receiving such information;

''(F) a review of the sharing of such information within the Federal Government to identify inappropriate stovepiping of shared information; and

''(G) any recommendations of the Inspector General of the Department of Homeland Security for improvements or modifications to the authorities under such section.

''(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under such subsection (b), shall annually and jointly submit to Congress a report assessing the privacy and

civil liberties impact of the activities conducted by the Federal Government under such section 1104. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under such section 1104.

''(3) FORM.—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

''(d) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Armed Services of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Armed Services of the Senate.

''(2) CYBER THREAT INFORMATION, CYBER THREAT INTELLIGENCE, CYBERSECURITY CRIMES, CYBERSECURITY PROVIDER, CYBERSECURITY PURPOSE, AND SELF-PROTECTED ENTITY.—The terms 'cyber threat information', 'cyber threat intelligence', 'cybersecurity crimes', 'cybersecurity provider', 'cybersecurity purpose', and 'self-protected entity' have the meaning given those terms in section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act.

''(3) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

''(4) SHARED SITUATIONAL AWARENESS.—The term 'shared situational awareness' means an environment where cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.''.

Page 5, strike line 6 and all that follows through page 6, line 7.

Page 7, beginning on line 17, strike ''by the department or agency of the Federal Government receiving such cyber threat information''.

Page 13, strike line 13 and all that follows through page 15, line 23.Page 17, strike line 15 and all that follows through page 19, line 19.

Page 17, strike line 15 and all that follows through page 19, line 19.

☒